Milestones of Cyber Security

Booz | Allen | Hamilton

Booz Allen Hamilton, a leading strategy and technology consulting firm, partners with clients to solve their most important and complex problems, making their mission our mission, and delivering results that endure. Booz Allen Hamilton has been a major player in cyber security for decades.

March 2009

The Great Cyber Awakening

Cyber Security, Information Assurance, Computer Security, Critical Infrastructure Protection—by whatever name, the protection of electronic information has become more necessary even as it has become more difficult.

The need to secure electronic information first arose as the early telegraphers began to define cyberspace with their dot- and dash-encoded messages. Today, increasingly frequent and visible cyber events—computer viruses, network denial of service attacks, cyber crime, and a host of others—have made cyber a “top of mind” issue throughout our society and the world.

This booklet is both a chronicle and a celebration of this fascinating field. The major milestones included here represent a weighty legacy—a legacy of accomplishment, of threat and countermeasure, of technological advance and cultural change.

As the milestones of the future unfold, they will mark our progress in addressing our cyber security challenges. Will we see improved business and mission outcomes as a result of improved security? resilient information systems that are resistant to degradation and that can be restored quickly in the aftermath of security incidents? and the broad emergence of norms of acceptable behavior in cyberspace? Such are the elements of the future to which we must aspire.

Booz | Allen | Hamilton

1940s

1942-43 Noted English mathematician and computer theorist Alan Turing designed the logic of the electromechanical device called the "bombe" to decrypt German military messages encrypted with the Enigma machine. The bombe was a variation of the original, which had been designed by Polish cryptologist Marian Rejewski.

1943 The discovery of a vulnerability involving the emanation of electronic signals from teletype encryption machines led to the development of TEMPEST rules and standards used by the United States to protect facilities and equipment from adversarial eavesdropping.

1943-44 One of the earliest programmable electronic computing devices, the Mark 2 Colossus, was developed and put into operational use by British codebreakers at Bletchley Park to decipher encrypted German teleprinter messages.

1945 The United States Army Security Agency was established to integrate the military's communications intelligence and communications security organizations under one command.

1949 Electrical engineer and mathematician Claude Shannon published *Communication Theory of Secrecy Systems*, a revised and declassified version of a paper he had written at Bell Labs in 1945, *A Mathematical Theory of Cryptography*. It provided the theoretical underpinning of modern cryptography. Shannon is now considered one of the founders of the Information Age for his work on communication theory.

Booz | Allen | Hamilton

1950s

1952 President Harry Truman established the National Security Agency (NSA) from a predecessor organization, the Armed Forces Security Agency (AFSA). The creation of NSA resulted from a study and report known as the "Brownell Report" after the chairman of a committee chartered by the Secretaries of State and Defense. The report surveyed the history of U.S. communications intelligence activities and suggested the need for a greater degree of coordination and direction at the national level.

1954 The first TEMPEST standard, MIL-STD-285, *Method of Attenuation Measurements for Enclosures, Electromagnetic Shielding, for Electronic Test Purposes*, was issued by the Department of Defense.

1957 Groundbreaking for the first Semi-Automatic Ground Environment (SAGE) site occurred at McCord AFB, WA. SAGE was an automated control system for tracking and intercepting enemy bombers. With 27 operations centers across the United States linked by telephone with over 100 air defense components, SAGE was the first wide-area computer network, and some of the pioneering technological advances it brought about are still in use today.

1958 In response to the USSR's launching of Sputnik, the first artificial earth satellite, in 1958, the U.S. Department of Defense established the Advanced Research Projects Agency (ARPA) with a focus on basic research to help the U.S. gain a lead in science and technology with military applications. ARPA's initial emphasis centered on space research (which was soon moved to the newly-formed National Aeronautics and Space Administration), ballistic missile defense, and nuclear test detection. ARPA began its computer science research program in 1961.

Booz | Allen | Hamilton

1960s

1963 President John F. Kennedy issued Executive Order 12472 to create the National Communications System, an interagency consortium of Federal departments and agencies whose representatives address Federal telecommunications assets and responsibilities.

1965 Development of the Multiplexed Information and Computing Service (Multics), the first programmable operating system to provide a hierarchical file structure managed by secure access control was begun. Multics provided a blueprint for the development of the modern operating systems commonly used by government, academic institutions, and industry.

1968 The Advanced Research Projects Agency developed a Program Plan entitled "Resource Sharing Computer Networks". The objectives of the program were to develop experience with the interconnection of computers and to improve and increase computer research productivity through resource sharing. Execution of this program plan led to development of ARPANET, the world's first operational packet switching network and the direct forerunner of today's Internet.

1969 Three members of the British Communications Headquarters invented the first set of asymmetric key algorithms, which would later be incorporated into a technique commonly referred to as 'non-secret encryption' or 'public-key cryptography.'

1970s

1970 RAND Report R-609, *Security Controls for Computer Systems* (also known as “The Ware Report”), was published to identify and recommend critical security protection mechanisms required to safeguard classified information stored in resource-sharing systems and included critical security standards and controls for such systems.

1971 IBM submitted its Lucifer block cipher algorithm to the National Bureau of Standards (NBS—predecessor organization to the National Institute of Standards and Technology—NIST) in response to an NBS request for proposals seeking a strong cryptographic algorithm to protect non-classified information. NBS adopted a modification of the Lucifer algorithm, which it released in 1976 as the Data Encryption Standard (DES).

1971 The first computer virus, known as ‘The Creeper’ was purposely designed and released on ARPANET. The virus gained access to ARPANET via the modem and copied itself to the remote system displaying the words: “I’m The Creeper: Catch me if you can.”

1972 The United States Air Force published *Preliminary Notes on the Design of Secure Military Computer Systems*, which not only espoused critical security design principles, but emphasized that the application of such principles would necessitate enhanced protection mechanisms and security assurances.

1972 The United States Air Force (USAF) published a report, written by information security pioneer, James P. Anderson, on the findings of a Computer Security Technology Planning

Study Panel. This panel was assembled to examine USAF multilevel computer security requirements and propose a research and development plan to guide work on open-use, multi-user, resource- sharing computer systems that process unclassified and classified information simultaneously in both secure and non-secure areas.

1972 The United States Department of Defense issued Directive 5200.28, *Security Requirements for Automatic Data Processing (ADP) Systems*, which established Federal policy for safeguarding classified, sensitive unclassified, and unclassified information within Automated Information Systems.

1973 The United States Department of Defense issued Manual 5200.28-M, *ADP Security Manual: Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, to prescribe guidelines for the implementation of Directive 5200.28 by all Defense departments and agencies.

1973 The first formal confidentiality model, the Bell-La Padula or BLP Model, was designed for government and military applications to categorize and enforce access control based on security levels. This model produced key conceptual tools that enhanced the security of time-sharing mainframe systems and ultimately formed the foundation for mandatory access controls.

1974 *Multics Security Evaluation, Volume II: Vulnerability Analysis* was published and reported on the potential use of Multics by the Air Force Data Services Center as a two-level (Secret/

Top Secret) system. Even though Multics did not meet certification requirements and standards, its highly-regarded security design principles proved useful for the development of a more certifiably-secure, multi-level system.

1975 “The Protection of Information in Computer Systems”, a widely-influential paper by Jerome Saltzer and Michael Schroeder of the Massachusetts Institute of Technology, appeared in the *Proceedings of the IEEE* (Institute of Electrical and Electronics Engineers). The paper articulated critical architectural structures required for sufficient information protection.

1975 Science fiction author John Brunner published his novel *Shockwave Rider* in which he invented the concept of network worms.

1976 Whitfield Diffie and Martin Hellman published their seminal paper “New Directions in Cryptography” outlining the concepts of public-key cryptography in the *IEEE Transactions on Information Theory*. This paper revolutionized cryptography research, fueling interest in researchers around the world.

1977 The U.S. General Accounting Office (now called the Government Accountability Office) published a draft *Guide for Evaluating Automated Systems* that provides auditors with a structured approach for evaluating an automated or computerized system. The approach placed primary emphasis on determining the reliability of the system being audited.

1977 Sen. Abraham A. Ribicoff (D-Conn.) introduced the *Federal Computer Systems Protection Act*, which sought to define "computer crimes" and recommended penalties for such crimes. The bill did not pass but did become a model for computer crime legislation at the State level and in other countries.

1977 A MITRE technical report by K.J. Biba for the United States Air Force, *Integrity Considerations for Secure Computer Systems*, describing a formal data integrity policy model, was published. The model, which became known as the Biba Integrity Model, described access constraints to protect data from improper modification.

1977 Three MIT researchers, Ronald Rivest, Adi Shamir, and Leonard Adleman discovered an elegant algorithm that enabled the practical implementation of public-key cryptography (called the RSA algorithm). The RSA breakthrough was first publicized by Martin Gardner in *Scientific American*.

1977 The United States Department of Defense established a Computer Security Initiative to increase the availability of trusted computer systems and to identify technical criteria and guidelines for evaluating the internal protection mechanisms of computer systems. Criteria proposed in the 1979 MITRE report, *Proposed Technical Evaluation Criteria for Trusted Computer Systems* (Grace H. Nibaldi, author), ultimately served to inform the Department of Defense's official Trusted Computer System Evaluation Criteria.

1978 The report *Secure Minicomputer Operating System (KSOS) Executive Summary: Phase 1: Design of the Department of Defense Kernelized Secure Operating System* was published to document the design and development of a marketable, practical, multi-level secure computer operating system.

1978 The Advanced Research Projects Agency (ARPA) Protection Analysis Project was completed. The project had been implemented to study operating system security vulnerabilities and identify possible automatable techniques for detecting such vulnerabilities in existing system software. The report's "pattern-directed protection evaluation" strategy was instrumental in identifying new security vulnerabilities within Multics.

1980s

1980 James P. Anderson published the report *Computer Security Threat Monitoring and Surveillance* on the findings of a study to improve computer system security auditing and surveillance capabilities. The concepts described in this report underpin automated misuse detection in mainframe systems.

1980 Richard J. Feiertag and Peter G. Neumann authored a report on the design of their Provably Secure Operating System (PSOS), which served as a valuable early model for hierarchically-layered abstraction as well as attestable security properties.

1980 The Naval Postgraduate School master's degree thesis of Philip A. Myers, *Subversion: The Neglected Aspect of Computer Security*, identified trap doors and Trojan Horses as the "most attractive" method of penetration for the serious attacker, and recommended life cycle protection of the security kernel in computer operating systems.

1982 Executive Order 12382 established the President's National Security Telecommunications Advisory Committee, an advisory body of key senior industry representatives assembled to provide national security and emergency preparedness communications policy expertise to the President.

1982 The first large-scale computer virus outbreak was caused by "Elk Cloner", a virus developed by a 15-year old high school student as a practical joke. Elk Cloner, a virus of a type that is now known as a boot sector virus, was spread by floppy disks and affected the Apple II operating system.

1983 The first version of the Trusted Computer Security Evaluation Criteria (TCSEC), the “Orange Book” was published. The Orange Book would become a Department of Defense security standard in 1985 and provide technical security guidance and associated system evaluation methodologies.

1984 The National Coordinating Center for Telecommunications, a joint industry and government operations center that coordinates the initiation, restoration, and reconstitution of the Nation’s foreign and domestic telecommunications services, was established.

1985 Neil Koblitz and Victor Miller independently proposed Elliptic Curve Cryptography (ECC)—the strongest public key cryptographic system known today. Due to its computational efficiency and low power requirements, ECC is well suited for applications such as smart cards, wireless communications, and other small devices.

1986 The first *Computer Fraud and Abuse Act* was passed defining Federal computer related crimes and associated penalties.

1986 Dorothy E. Denning reported on the development of the first model of a real-time Intrusion Detection System at the 1986 IEEE Symposium on Security and Privacy. Commonly referred to as the Intrusion Detection Expert System, the model was based on the hypothesis that security violations can be detected by monitoring a system’s audit records for abnormal patterns of system usage.

1986 Astronomer Clifford Stoll played a pivotal role in methodically tracking down a hacker who had penetrated computer systems at Lawrence Berkeley National Laboratory. Stoll described these events in his 1990 book *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*.

1987 The United States Congress passed the *Computer Security Act of 1987* to promote the establishment of minimum security practices for Federal computer systems, the development of enhanced computer security plans for sensitive information, and computer security awareness training. The act, which was signed into law, assigned to the National Bureau of Standards (now the National Institute of Standards and Technology) the mission of developing security standards, guidelines, and associated methods and techniques for computer systems.

1987 David Clark and David Wilson presented *A Comparison of Commercial and Military Computer Security Policies* at the 1987 IEEE Symposium on Research in Security and Privacy that defined a new formal model for data integrity enforcement. The Clark-Wilson model is designed to be more applicable to business systems than the multi-level security needs of military systems.

1987 Ronald Rivest of RSA Security created Rivest Cipher 4 (RC4), a symmetric encryption algorithm that was subsequently adopted as the standard encryption algorithm in SSL (Secure Sockets Layer) and WEP (Wired Equivalent Privacy) applications.

1988 Robert Morris, a 23-year old doctoral student at Cornell University, released what became known as the Morris Worm, virtually paralyzing the Internet. Morris was later tried and convicted of violating the 1986 *Computer Fraud and Abuse Act*.

1988 Following the release and global impact of the Morris Worm, Carnegie Mellon University founded a Computer Emergency Response Team Coordination Center (CERT/CC) to maintain communications during security incidents and to mitigate future Internet security problems.

1988 The first packet filtering firewall technology was developed, a first-generation technical security feature for the Internet.

1988 The Massachusetts Institute of Technology invented Kerberos, a network authentication protocol designed to provide strong authentication for client/server application that uses secret key cryptography.

1989 David F.C. Brewer and Michael J. Nash published *The Chinese Wall Security Policy* at the 1989 IEEE Symposium on Research in Security and Privacy. The Chinese Wall (or Brewer-Nash) security model combined commercial discretionary and legally-enforceable mandatory controls. It was considered to be as significant to the financial world as Bell-LaPadula model was to military systems.

1989 Rep. Edward Markey (D-Mass.) introduced the *Computer Network Protection Act of 1989 (HR 3524)*, a bill that proposed amending the *Communications Act of 1934* to protect computer owners and telecommunications carriers, and discourage the propagation of computer viruses. The bill was referred to committee and never brought to a vote.

1989-90 The circuit level firewall, a second-generation architecture, was developed, as was the implementation of the first working model of the application layer firewall, a third-generation architecture.

1990s

1990 The United Kingdom, the Netherlands, Germany, and France jointly published the first compilation of guidelines for assessing computer products and systems security also known as the *Information Technology Security Evaluation Criteria*.

1990 The Trusted System Interoperability Group (TSIG), a consortium of computer systems vendors developing protocols for trusted systems, was formed to define interoperability protocols and guidelines for demonstrating that viable products capable of implementing multi-level security (MLS) were interoperable.

1990 Mitch Kapor, John Perry Barlow, and John Gilmore formed the Electronic Freedom Foundation (EFF) to work on civil liberties issues raised by new digital technologies. EFF, a nonprofit advocacy organization, champions free speech, privacy, innovation, and consumer rights.

1990 A joint government-industry collaborative effort led to the implementation of a Telecommunications Service Priority Program that provides national security and emergency preparedness users with priority authorization of telecommunications services.

1990-91 The Digital Equipment Corporation produced the first commercial application layer or proxy-based firewall called the Secure External Access Link product.

1991 *Computers at Risk: Safe Computing In the Information Age* was published by the National Research Council. This seminal work was a clarion call for action on developing computer technology that would support substantially increased safety, reliability, and, in particular, security.

1991 The creation of the Government Emergency Telecommunications Service, an emergency phone service provided by the National Communications System to support Federal, State, local, and tribal government, industry, and non-governmental organization personnel in performing their national security and emergency preparedness missions.

1991 The Network Security Information Exchange was formed. It is a joint industry-government body that imparts sensitive threat information to operations, administration, maintenance, and provisioning systems sustaining the telecommunications infrastructure.

1991 The Defense Intelligence Agency issued Manual 50-4, *Compartmented Mode Workstation (CMW) Evaluation Criteria,* Version I, to describe minimum security requirements for standard encodings of security labels in compliance with the Compartmented Mode.

1991 Philip Zimmermann created Pretty Good Privacy (PGP), an email encryption software package, and published it free on the Internet. Zimmerman's action was in response to United States Senate Bill 266 (defeated) designed to force manufacturers of secure communications products to provide a "back door" by which the United States Government would be able to read the communication.

1991 Bill Cheswick and Steve Bellovin began researching dynamic packet filtering and went so far as to help develop an internal firewall product at Bell Laboratories based upon this architecture; however, this product was never released.

1992 The Federal Criteria was an attempt to develop criteria to replace the TCSEC. A draft version was released for public comment in December 1992. However, this effort was supplanted by the Common Criteria effort, and the Federal Criteria never moved beyond the draft stage (although many of its ideas are retained in the Common Criteria).

1992 Bob Braden and Annette DeSchon at the University of Southern California's Information Sciences Institute began independently researching dynamic packet filter firewalls for a system that they called "Visas".

1993 The first Internet Firewall Toolkit is developed for constructing and managing network firewalls from a freely available set of tools.

1993 Computer security professionals, government employees, and others with an interest in computer code and architecture came together for the first annual DEFCON Hacker Convention in Las Vegas, Nevada.

1993 Major commercial-off-the-shelf relational database management system vendors initiated the release of multi-level security (MLS) versions of their databases such as Trusted Oracle7, Sybase Secure SQL Server, and Informix Online/Secure.

1994 Check Point Software Technologies Ltd. released FireWall-1, the first commercial software to use stateful inspection.

1994 The *Communications Assistance for Law Enforcement Act* (CALEA) was signed into law. It defined statutory requirements for telecommunications carriers to aid law enforcement in the implementation of electronic surveillance.

1994 Netscape Communications designed and implemented Secure Sockets Layer or SSL, a protocol enabling secure electronic commerce transactions, which gave a major boost to the conduct of online business. SSL was included in early versions of the Netscape Navigator browser.

1994 The first Internet Security Scanner, a shareware product pioneered and developed by Christopher Klaus, was publicly released.

1995 Wheelgroup Corporation commercialized the United States Air Force's security prototype called Netranger, a network configuration and information toolkit that scans traffic for signature misuse.

1996 Rep. Stephen Horn (R-Calif.), chairman of a House Government Reform subcommittee, published his first quarterly *Year 2000 Readiness Report Card* for Federal agencies to draw attention to potential computer problems associated with the Year 2000 rollover. Many agencies received failing grades.

1996 The President's Commission on Critical Infrastructure Protection was established to safeguard and assure the survivability of the Nation's vital infrastructure systems against physical and cyber threats.

1996 The Common Criteria (CC) for Information Technology Security Evaluation was published. The CC was produced by unifying pre-existing evaluation criteria (Trusted Computer System Evaluation Criteria—TCSEC, Information Technology Security Evaluation Criteria—ITSEC, and Canadian Trusted Computer Product Evaluation Criteria—CTCPEC) so that companies selling computer products for the government market would only need to have them evaluated against one set of standards. The CC was developed by the governments of Canada, France, Germany, the Netherlands, the United Kingdom, and the United States.

1996 The first version of the System Security Engineering Capability Maturity Model (SSE-CMM) was released. Based on the System Engineering Capability Maturity Model, SSE-CMM identifies both the unique characteristics of security engineering, and the integration of security activities into the overall system engineering process.

1997 Cisco released the first commercial Centri Firewall based on fifth generation firewall architecture.

1997 The White House Office of Science and Technology Policy released the report *CYBERNATION: The American Infrastructure in the Information Age*. The report articulated the technical and policy issues of critical infrastructure protection.

1998 President Bill Clinton issued Presidential Decision Directive 63 (PDD 63), *Critical Infrastructure Protection*, which declared the intent to take all necessary measures to eliminate any significant vulnerability to physical or cyber attacks on critical infrastructures, including cyber systems. PDD 63 led to the creation of multiple Information Sharing and Analysis Centers—privately-owned operational entities used to foster government-industry partnerships by sharing critical threat, vulnerability, intrusion, and solutions information.

1998 The *Digital Millennium Copyright Act* (DCMA) was signed into law making it illegal to manufacture and distribute technology, devices, or services intended to evade measures that control access to copyrighted products.

1998 Sponsored by the U.S. government, the Common Vulnerabilities and Exposures (CVE) dictionary was developed and launched. CVE is a "common enumeration" of community-shared information security vulnerabilities and mitigation strategies, and in time became the industry standard for vulnerability and exposure names.

1998 Department of Defense computer systems sustained a series of attacks that appeared to be from multiple countries, including Israel, the United Arab Emirates, France, Taiwan, and Germany. These events, given the name "SOLAR SUNRISE", coincided with U.S. preparation for possible military operations in the Balkans, leading to the incorrect perception that a politically-motivated coordinated attack was underway. It was ultimately determined to be the work of two teenagers under the tutelage of an Israeli hacker.

1998 United States Department of Defense established a Joint Task Force on Computer Network Defense to serve as the focal point for the Department's components to collectively defend their computer networks and systems.

1998 Martin Roesch released Snort, a free lightweight Intrusion Detection System for UNIX systems.

1999 The Electronic Freedom Foundation and Distributed.net, a worldwide coalition of computer enthusiasts, cracked the 56-bit Data Encryption Standard (DES) code in less than 23 hours. The previous record had been 39 days. EFF and Distributed.net were awarded a $10,000 prize offered by RSA Data Security to anyone who broke DES in under 24 hours.

1999 The Department of Defense issued Directive 5144.1, *NetOps for the Global Information Grid*, which establishes guidance and designates responsibility for implementing and executing NetOps so as to maintain and protect the Global Information Grid.

1999 The National Institute of Standards and Technology (NIST) announced that the 56-bit Data Encryption Standard (DES) was no longer sufficient and recommended the use of Triple-DES.

Booz | Allen | Hamilton

2000s

2000 A spate of distributed denial of service (DDoS) attacks temporarily brought down several of the world's largest and most popular portal and e-commerce sites. The attacks prompted Congressional hearings and legislative proposals aimed at closing security holes and intensifying the hunt for cyber vandals.

2000 The Clinton Administration released the *National Plan for Information Systems Protection*, the first-ever national cyber strategy aimed to secure the Nation's computer networks from future cyber attacks.

2000 The SANS Institute and the National Infrastructure Protection Center released the *Ten Most Critical Security Vulnerabilities*, a consensus-driven compilation of the most critical security vulnerabilities.

2000 The Council of Europe drafted a *Cybercrime Treaty* to promote the international harmonization of laws against computer crimes.

2000 The Wireless Priority Service, a national security program for priority cellular telephone service that provides an end-to-end priority communications capability during natural emergencies or man-made disasters, was created.

2001 The Open Web Application Security Project (OWASP) was founded. OWASP is a worldwide free and open community focused on improving the security of application software through enhanced visibility of security risks.

2001 Congress conducted its second annual review of computer security at Federal agencies. The agencies received a collective score of “D-minus.” The White House Office of Management and Budget promised to withhold funding for Federal information technology programs that do not improve security.

2002 Official release of the Open Vulnerability and Assessment Language, a globally-accepted information security standard developed to promote the sharing of public security information and to regulate the movement of this information across security tools and services.

2002 The *Federal Information Security Management Act* (FISMA) was passed to promote the adoption of critical security standards and guidelines by all Federal departments and agencies.

2002 The National Institute of Standards and Technology (NIST) reported rapid adoption of the Advanced Encryption Standard (AES), which would become the nationally-approved algorithm for securing sensitive but unclassified information.

2002 A distributed denial of service (DDoS) attack struck the 13 Domain Name System (DNS) root servers knocking out all but five. This was the first attempt to disable the Internet itself rather than individual hosts or enclaves.

2003-05 A series of coordinated attacks on the computer systems of the U.S. Department of Defense, other U.S. government agencies, defense contractors, and other private sector organizations were widely believed to have originated in China. The attacks, collectively referred to by the term “Titan Rain”, were conducted with precision and discipline, leading to speculation that they were orchestrated by a military organization. Contemporaneous reporting indicated that hackers left back doors for repeated entry.

2003 United States Congress passed the *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act* to regulate commercial email traffic by imposing limitations and penalties on those who sent unsolicited mail via the Internet.

2003 *The National Strategy to Secure Cyberspace* was published to promote a nation-wide effort to secure U.S.-owned, operated, and controlled portions of cyberspace by preventing cyber attacks, reducing national vulnerabilities, minimizing damage, and maximizing reconstitution capabilities.

2003 The United States Computer Emergency Readiness Team (US-CERT) was created to provide response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS). It is a public-private partnership.

2004 Software Assurance (SwA) Program of the Department of Homeland Security National Cyber Security Division was formed. SwA is a strategic unit designed to develop practical guidance and tools for the promotion of research and development investment in cybersecurity. SwA launched “Build Security In”, a strategic initiative developed to provide a variety of physical and regulatory resources for making software more secure.

2004 The Jericho Forum was created by a group of global corporate Chief Information Security Officers to influence development of secure architectures, technology solutions to enable secure global collaboration between enterprises. The Jericho Forum operates under the auspices of The Open Group, a vendor- and technology-neutral non-profit consortium dedicated to enabling access to information based on open standards and global interoperability.

2005 The Computer Security Institute published its first annual *Computer Crime and Security Survey*, which would become the most widely-referenced security research around the globe.

2007 The White House Office of Management and Budget established the Trusted Internet Connections initiative to reduce all government external connections to Internet Service Providers to a target of 50 connections; this includes both Internet and telecommunications lines.

2007 The nation of Estonia was the victim of a series of cyber attacks that targeted Estonian government, banking, media, and police websites. Most of the attacks were distributed denial of service attacks—both elementary methods such as ping floods as well as more sophisticated botnets. Amid speculation that the attacks were state-sponsored, no positive attribution of the attackers was determined.

2007 A distributed denial of service (DDoS) attack struck the 13 Domain Name System (DNS) root servers knocking out all but five. This was the first attempt to disable the Internet itself rather than individual hosts or enclaves.

2007 The Beta version of the Security Content Automation Protocol (SCAP) was released. SCAP is a technique for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. It consists of a suite of selected open standards that enumerate software flaws, security related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to score the results of these measurements in order to evaluate the impact of the discovered security issues.

2007 The Department of Defense (DoD) issued the DoDD 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, establishing a certification and accreditation (C&A) process to manage the implementation of information assurance capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD information systems. DIACAP emphasized enterprise and life cycle management of system security.

2008 National Security Presidential Directive 54/Homeland Security Presidential Directive 23 formalized the Comprehensive National Cybersecurity Initiative (CNCI), intended to establish a frontline defense against a full spectrum of cyber threats.

2008 The National Cyber Security Division of the U.S. Department of Homeland Security released the Common Attack Pattern Enumeration and Classification (CAPEC) resource, a publicly-accessible taxonomy of attack patterns.

2008 Sponsored by the U.S. government, the Common Weaknesses Enumeration (CWE) dictionary was developed and launched. CWE is a community-developed formal list of software weakness types used to identify, mitigate, and prevent software security flaws.

Booz | Allen | Hamilton